PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference FP1782	FOR FURTHER ACTION	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)

International application No. PCT/SG 2002/000227	International filing date (day/month/year) 4 October 2002 (04.10.2002)	Priority Date (day/month/year) 31 July 2002 (31.07.2002)

International Patent Classification (IPC) or national classification and IPC
IPC[7]: G06F12/14, G11C16/22, G11C11/412

Applicant
TREK 2000 INTERNATIONAL LTD

1. This international preliminary examination report has been prepared by this International Preliminary Examination Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of __3__ sheets, including this cover sheet.

☒ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of __3__ sheets.

3. This report contains indications relating to the following items:

   I. ☒ Basis of the opinion

   II. ☐ Priority

   III. ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability

   IV. ☐ Lack of unity of invention

   V. ☒ Reasoned statement under Rule 66.2(a)(ii) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

   VI. ☐ Certain documents cited

   VII. ☐ Certain defects in the international application

   VIII. ☐ Certain observations on the international application

Date of submission of the demand 17.12.2003	Date of completion of this report 1 March 2005 (01.03.2005)

Name and mailing address of the IPEA/AT Austrian Patent Office Dresdner Straße 87 A-1200 Vienna Facsimile No. 1/53424/200	Authorized officer HARASEK S. Telephone No. 1/53424/574

Form PCT/IPEA/409 (cover sheet) (July 1998)

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

I.	Basis of the report

1. With regard to the **elements** of the international application:*

☐ the international application as originally filed

☒ the description:
pages _1-13_ , as originally filed
pages _____ , filed with the demand
pages _____ , filed with the letter of _____ .

☒ the claims:
pages _15_ , as originally filed
pages _____ , as amended (together with any statement) under Article 19
pages _____ , filed with the demand
pages _14, 16, 17_ , filed with the letter of _4 February 2005 (04.02.2005)._

☒ the drawings:
pages _1-7_ , as originally filed
pages _____ , filed with the demand
pages _____ , filed with the letter of _____ .

☐ the sequence listing part of the description:
pages _____ , as originally filed
pages _____ , filed with the demand
pages _____ , filed with the letter of _____ .

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.
These elements were available or furnished to this Authority in the following language _____ which is:

☐ the language of a translation furnished for the purposes of international search (under Rule 23.1(b)).

☐ the language of publication of the international application (under Rule 48.3(b)).

☐ the language of the translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/ or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

☐ contained in the international application in printed form.

☐ filed together with the international application in computer readable form.

☐ furnished subsequently to this Authority in written form.

☐ furnished subsequently to this Authority in computer readable form.

☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. ☒ The amendments have resulted in the cancellation of:

☐ the description, pages _____ .

☒ the claims, Nos. _21, 22._

☐ the drawings, sheets/fig _____ .

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).**

Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as „originally filed" and are not annexed to this report since they do not contain amendments (Rules 70.16 and 70.17).

** Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.*

Form PCT/IPEA/409 (Box I) (July 1998))

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1-20		YES
	Claims	____		NO
Inventive step (IS)	Claims	1-20		YES
	Claims	____		NO
Industrial applicability (IA)	Claims	1-20		YES
	Claims	____		NO

Citations and explanations (Rule 70.7)

The following documents have been cited in the Search Report:

D1: WO1995/016238A1
D2: EP1085521A1
D3: US5469564A
D4: JP2002222022A

Documents D1-D3 deal with data storage devices featuring provisions for controlled access to stored data. D4, in turn, shows an electronic appliance equipped with an automatic shutdown algorithm executable upon the attempt of unauthorised use.

Document D1 is considered to form the closest state of the art regarding the present application. Some of the most relevant features of claim 1, such as an authentication sequence and algorithm being stored in a read-only memory and the presence of a logic circuit for the execution of the authentication process of a received password in order to grant or deny access to stored data are explicitly mentioned.

However, with the amendments of the claims additional features – which are within the scope of the initial disclosure - have been added to claim 1. One of these features concerns the encryption of received data in the device before usage of the data in the host and is not disclosed in any of the cited documents. Claim 1 is therefore regarded inventive in view of the state of the art.

Accordingly, also the claims 2-17 dependent on claim 1 can now be considered involving an inventive step as well as claims 18-20 have already been before.

Summarising, all claims are now after amendment regarded to be novel and involving an inventive step. Industrial applicability is given.

CLAIMS

1.   An authentication system to verify a password, the system being arranged for coupling to a host for communication therewith, and comprising:

a first storage unit to store an authentication sequence;

5   a read-only memory unit to store an authentication algorithm;

a microcontroller coupled to said first storage unit, said read-only memory unit, and a web server, wherein said microcontroller is to receive said password and execute said authentication algorithm and wherein said authentication algorithm is to verify said password with said authentication sequence; and

10   a second storage unit coupled to said microcontroller to store data from said web server and wherein access to said second storage unit is permitted by said microcontroller only if said password has been verified,

wherein the system is arranged to receive data from the web server, via the host, in encrypted form and to decrypt that data before use thereof in the host.

15

2.   The authentication system as recited in claim 1, wherein the password is received by said microcontroller from said host.

3.   The authentication system as recited in claim 2, wherein said read-only
20   memory unit further comprises a shutdown algorithm to shut down said host and said authentication system after a number of incorrect passwords is received by said microcontroller.

4.   The authentication system as recited in claim 2, wherein said password is received by said host from said web server.
25

5.   The authentication system as recited in claim 2, wherein said authentication algorithm is hard coded on one of a group consisting of a firmware and a hardware in said microcontroller.

AMENDED SHEET

14.   The authentication system as recited in claim 12, wherein said authentication sequence is hash-coded.

5   15. ·   The authentication system as recited in claim 1, wherein said first storage unit is located within said read-only memory unit and wherein said authentication sequence is hard coded into said first storage unit.

16.   The authentication system as recited in claim 15, wherein said second storage area further comprises a public storage area and a private storage area.

17.   The authentication system as recited in claim 16, wherein said first storage unit is located within said private storage area of said second storage area.

15   18.   A method for authenticating a password, comprising:
coupling an authentication system to a host for communication therewith;
the system receiving said password;
the system receiving data from a web server, via the host, in encrypted form, wherein said data is stored in a storage unit of the system;
the system providing an authentication sequence;
20   the system executing an authentication algorithm to verify said password with said authentication sequence, wherein said authentication algorithm is stored on a read-only memory unit of the system;
the system permitting access to said data on said storage unit only if said password is verified; and
the system decrypting the data before use in the host.

25

19.   The method for authenticating a password as recited in claim 18, wherein said password is received from said web server.

20.   The method for authenticating a password as recited in claim 19, wherein said password is entered by a user.